IN THE CLAIMS:

Amended claims follow:

1. (Cancelled)

2. (Currently Amended) ~~A method according to claim 1,~~A method for generating an authentication tag for a message, comprising:

processing a portion of the message using a first function to produce an interim output; and

processing the interim output using a second function to produce the authentication tag;

wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by using a pseudorandom probabilistic function to determine whether each message part is provided as input to said first function.

3. (Original) The method of claim 2, wherein said message parts are 64-bit words.

4. (Currently Amended) ~~A method according to claim 1, further comprising~~A method for generating an authentication tag for a message, comprising:

processing a portion of the message using a first function to produce an interim output;

processing the interim output using a second function to produce the authentication tag; and

partitioning the message into regions, each region including a number of message parts, and providing one message part from each region as input to said first function.

5. (Currently Amended) ~~A method according to claim 1,~~A method for generating an authentication tag for a message, comprising:

processing a portion of the message using a first function to produce an interim output; and

processing the interim output using a second function to produce the authentication tag;

wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by:

defining a message selection percentage p; and

using a pseudorandom probabilistic function, uniform over an interval [1, 2L], where L = 1/p and p is a message selection percentage, to determine offsets between message parts which are provided as input to said first function.

6. (Currently Amended) ~~A method according to claim 1,~~A method for generating an authentication tag for a message, comprising:

processing a portion of the message using a first function to produce an interim output; and

processing the interim output using a second function to produce the authentication tag;

wherein said first function is a keyed hash function.

7. (Currently Amended) ~~A method according to claim 1,~~A method for generating an authentication tag for a message, comprising:

processing a portion of the message using a first function to produce an interim output; and

processing the interim output using a second function to produce the authentication tag;

wherein the ~~cryptographic hash~~first function is one of an MD4 hashing function, a bucket hashing function, a multilinear modular hashing function, a cyclic redundancy code-based hashing function, and an alternative hash algorithm.

8. (Currently Amended) ~~A method according to claim 1,~~A method for generating an authentication tag for a message, comprising:

processing a portion of the message using a first function to produce an interim output; and

processing the interim output using a second function to produce the authentication tag;

wherein the portion of the message processed is selected by truncating the message.

9. (Cancelled)

10. (Currently Amended) ~~A device according to claim 9,~~A device for generating an authentication tag for a message, comprising:

a first hashing module that processes a portion of the message to produce an interim output; and

a second hashing module that processes said interim output to produce the authentication tag;

wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by using a pseudorandom probabilistic function to determine whether each message part is provided as input to said first hashing module.

11. (Original) The device of claim 10, wherein said message parts are 64-bit words.

12. (Currently Amended) ~~A device according to claim 9, further comprising partitioning~~A device for generating an authentication tag for a message, comprising:

a first hashing module that processes a portion of the message to produce an interim output; and

a second hashing module that processes said interim output to produce the authentication tag;

wherein the message is partitioned into regions, each region including a number of message parts, and ~~providing~~ one message part from each region is provided as input to said first hashing module.

a1

13. (Currently Amended) ~~A device according to claim 9,~~A device for generating an authentication tag for a message, comprising:

a first hashing module that processes a portion of the message to produce an interim output; and

a second hashing module that processes said interim output to produce the authentication tag;

wherein the message includes a number of message parts, and wherein the portion of the message processed is selected by:

defining a message selection percentage p; and

using a pseudorandom probabilistic function, uniform over an interval [1, 2L], where L = 1/p and p is a message selection percentage, to determine offsets between message parts which are provided as input to said first hashing module.

14. (Currently Amended) ~~A device according to claim 1,~~A device for generating an authentication tag for a message, comprising:

a first hashing module that processes a portion of the message to produce an interim output; and

a second hashing module that processes said interim output to produce the authentication tag;

wherein said first hashing module includes a keyed hash function.

15. (Currently Amended) ~~A device according to claim 1,~~A device for generating an authentication tag for a message, comprising:

a first hashing module that processes a portion of the message to produce an interim output; and

a second hashing module that processes said interim output to produce the authentication tag;

wherein said first hashing module includes one of an MD4 hashing function, a bucket hashing function, a multilinear modular hashing function, a cyclic redundancy code-based hashing function, and an alternative hash algorithm.

16. (Currently Amended) ~~A device according to claim 1,~~A device for generating an authentication tag for a message, comprising:

a first hashing module that processes a portion of the message to produce an interim output; and

a second hashing module that processes said interim output to produce the authentication tag;

wherein the portion of the message processed is selected by truncating the message.